Donau-Universität Krems
Zentrum General Management & Corporate Programs
Dr.-Karl-Dorrek-Str. 30
3500 Krems

New Economy – Challenges and Approach

IT-Sicherheitsfragen bei internationalen Vertragsabschlüssen im e-Commerce

Betreuer: ao. Univ.-Prof. Mag. Dr. Siegfried Fina,

Rechtliche Rahmenbedingungen für e-Commerce in Europa

Dipl.-Ing. Gerhard Müller

Wien, am 13. Mai 2002

Zusammenfassung

Von grundlegender Bedeutung für die Weiterentwicklung des e-Commerce sind Sicherheitsfragen bei der Abwicklung der Vertragsabschlüsse über das Internet. Diese Fragen betreffen sowohl den B2C- als auch den B2B-Bereich und werden hauptsächlich über die Einführung elektronischer Signaturen beantwortet. Elektronisch abgeschlossene Rechtsgeschäfte passen zwar prinzipiell in den rechtlichen Kontext übereinstimmender Willenserklärungen, sind aber durch die inhärente technische Offenheit des Internet für Manipulationen nicht abgesichert. Das bezieht sich sowohl auf die Authentizität der beteiligten Parteien als auch auf die Integrität der Willenserklärungen. Die Anwendung elektronischer Signaturen kann diese Probleme größtenteils lösen, allerdings bleiben einige technische Detailfragen offen, die auf der Ebene von Einzelfällen von den Gerichten zu klären sein werden. Diese Arbeit konzentriert sich hauptsächlich auf die EU-Signaturrichtlinie und deren Umsetzung in österreichisches Recht. Vergleiche mit dem US-amerikanischen Rechtsansatz zeigen einige Differenzen auf. Der amerikanische E-Sign Act macht etwa keinerlei Vorschriften bezüglich der technischen Umsetzung von Signatursystemen, während die EU-Signaturrichtlinie zumindest fortgeschrittene elektronische Signaturen relativ genau regelt. Die Kompatibilität der Rechtsordnungen ist daher bei transatlantischen Rechtsgeschäften derzeit noch fraglich, obwohl viele Bemühungen in Richtung international einheitlicher Regelungen gehen (z.B. UN-Modellgesetz über elektronische Signaturen).

Inhaltsverzeichnis

Abkürzungsverzeichnis

AGB	Allgemeine Geschäftsbedinungen
ASCII	American Standards Code for Information Interchange, generisches Datenformat für die Textdarstellung auf Rechenanlagen
B2B	„Business to Business“-Beziehung zwischen Unternehmen, Geschäftsprozesse laufen über das Internet.
B2C	„Business to Consumer“-Beziehung zwischen Unternehmen und Konsumenten, die ihrerseits auch Unternehmen sein können.
BG	Bundesgesetz
BGBl	Bundesgesetzblatt
EVÜ	Europäisches Vertragsstatut Übereinkommen
HTML	Hypertext Markup Language, gebräuchlichstes Dokumentformat im WWW
IPRG	Gebräuchliche Abkürzung für das Bundesgesetz über das internationale Privatrecht.
ÖVE	Österreichischer Verband für Elektrotechnik
PDF	Portable Document Format, Dokumentformat der Firma Adobe
PIN	Personal Identification Number, Passwort für Kreditkarten, Chipkarten, etc.
RSA	Asymmetrisches Verschlüsselungsverfahren nach Rivest/Shamir/Adleman
RTR	Rundfunk- und Telekom Regulierungs GmbH
SET	„Secure Electronic Transaction“, sichere Transaktionen über Kreditkartenunternehmen, Authentifizierung und Verschlüsselung der Daten.
TAN	Transaktionsnummer, einmaliger Schlüssel für Online-Banking
TKK,TKC	Telekom-Control-Kommission
UNCITRAL	United Nations Commission on International Trade Law
WWW	„World Wide Web“, das Internet.
ZPO	Zivilprozessordnung

1 Vertragsabschlüsse im Internet

1.1 Die Willenserklärung[1]

Grundlegend für das Zustandekommen von Rechtsgeschäften ist der Abschluss eines Vertrags zwischen den beiden Parteien, d.h. dem Anbieter von Waren bzw. Dienstleistungen im Internet und dem Kunden („User"). Nach österreichischem Recht (§861 ABGB) kommt ein Vertrag durch den übereinstimmenden Willen der Vertragsparteien zustande, d.h. eine der beiden Parteien macht ein Versprechen, das durch den anderen Teil angenommen wird. Willenserklärungen können nach §863 ABGB auch stillschweigend durch Handlungen abgegeben werden, deren Interpretation zweifelsfrei mit Rücksicht auf Gebräuche und Gewohnheiten sein muss. Damit ist (zumindest nach österreichischem Recht) der Grundstein für Vertragsabschlüsse im Internet gelegt und es wäre lediglich im zeitlichen Ablauf der Prozess Angebot ⇒ Annahmefrist ⇒ Annahme von den Vertragsparteien einzuhalten.

1.1.1 Angebot

Ein rechtsverbindliches Angebot („Offerte") muss inhaltlich bestimmt sein und den endgültigen Bindungswillen des Antragstellers zum Ausdruck bringen. Grundsätzlich gilt daher die Webseite eines „e-Shops", ähnlich Prospekten oder Produktkatalogen, nicht als Angebot, da aus Sicht des Betreibers der Webseite nicht unbedingt sichtbar ist, wer zu welchem Zeitpunkt Waren oder Dienstleistungen bestellen will und wie die Relation zu den Lagerbeständen zu sehen ist.[2] Daher geht das Angebot regelmäßig vom Benutzer der Webseite aus und ist erst danach vom Webseitenbetreiber anzunehmen.

1.1.2 Annahmefrist und Annahme

Nach Absendung des Angebots durch den Benutzer beginnt eine vereinbarte bzw. „angemessene" Annahmefrist zu laufen, während der grundsätzlich nach §862 ABGB die Annahme zu erfolgen hat. Eine verspätet abgesendete Annahmeerklärung gilt dann als neues Angebot seitens des Webseitenbetreibers, das vom Benutzer wiederum (auch konkludent) angenommen werden kann.

1.2 Rücktritt vom Vertrag

Auch wenn nun augenscheinlich ein rechtsgültiger Vertrag durch Angebot und Annahme zustande gekommen ist, könnte dieser etwa durch die Irrtumsregelungen der §§ 871 ABGB nichtig werden. Im *B2C*-Bereich ist ein Rücktritt binnen einer Woche nach §3 KSchG eher zu

[1] Podovsovnik, G.; Neubauer, P.; Toch, R.: Der Vertragsabschluss im Internet. In: Aktuelle Rechtsfragen des Internets. Hrsg.: W. Lattenmayer; A. Behm. Wien: Manz, 2001. S. 70 ff.

[2] Ausnahmen bestehen hier etwa durch integrierte elektronische Lagerverwaltung oder Verkauf von Software, Bildern und Videos, etc. die zum „download" angeboten werden. Auch können die Benutzer des e-Shops durchaus bekannt sein und damit ein verbindliches Anbot in Form der Webseite begründen.

verneinen, da der Benutzer selbst das Rechtsgeschäft angebahnt hat, allerdings kann nach der „Fernabsatzrichtlinie“ ein Verbraucher auch nach Vertragsabschluss[3] binnen mindestens 7 Werktagen vom Vertrag zurücktreten[4].

1.3 Willenserklärungen über Computer

Gerade im e-Commerce laufen einzelne Teile des Prozesses vom Anbot bis zur Annahme über Software, wie etwa die Anbotsannahme durch eine Webseite. Diese Software übernimmt dabei die Aufgaben eines Gehilfen, sodass die automatisch generierten Willenserklärungen dem Webseitenbetreiber zuzurechnen und auch rechtsverbindlich sind. Der Benutzer kann auf der anderen Seite mit seiner Bestellung im Irrtum sein, womit wiederum die Irrtumsregeln des ABGB greifen (§871 ABGB). Daher sind bei dieser Software Mechanismen vorzusehen, die Plausibilitäten der Bestellung prüfen oder Rückbestätigungen des Benutzers einholen.

1.3.1 Authentizität der Vertragspartner

Jedenfalls stellt sich bei Willenserklärungen über das Internet die Frage nach der Authentizität der Vertragspartner, um überhaupt ein Rechtsgeschäft abwickeln zu können. Bisherige Praxis in Bezug auf Zahlung mit Kreditkarte im Internet war einfach der Verzicht auf die (technisch kompliziertere) elektronische Authentifizierung des Karteninhabers und Übernahme etwaiger Schäden durch die Kreditkartenfirmen, falls Kartendaten missbräuchlich verwendet wurden. Für *B2C*-Rechtsgeschäfte gilt insbesondere §31a KSchG, der für solche Fälle zwingend die Rückerstattung geleisteter Zahlungen durch das Kreditkartenunternehmen vorschreibt.[5]

1.3.2 Integrität der Bestelldaten

Auch die Integrität des Inhalts von Willenserklärungen ist im Internet technisch beliebig verfälschbar wenn keine oder unzureichende Verschlüsselungsmethoden angewendet werden. Mit der Einführung von „sicheren“ Webseiten, die eine verschlüsselte Kommunikation zwischen Benutzern und Webseitenbetreibern erlauben, wurde ein wichtiger Schritt in Richtung Integrität des Datenaustausches getan. Damit wurde auch das „Mitschneiden“, d.h. unerlaubte Kopieren von Kreditkartennummern zumindest erschwert (siehe auch 3.2).

1.4 US-amerikanisches Vertragsrecht

Die amerikanische Vertragsinterpretation beruht allgemein auf Versprechungen und deren Erfüllung und umfasst nicht jede auf Anbot und Annahme basierende Willensübereinkunft. Der Vertragsabschluss erfolgt ebenfalls auf Anbot und Annahme, allerdings gibt es große Unterschiede zum österreichischen und deutschen Vertragsrecht. So ist z.B. die

[3] mit Ausnahmen, wie z.B. verderbliche Waren, Waren nach Kundenspezifikation, entsiegelte Softwareprodukte, etc.
[4] Artikel 6 Fernabsatzrichtlinie 97/7/EG
[5] Podovsovnik, G.; Neubauer, P.; Toch, R.: Der Vertragsabschluss im Internet. In: Aktuelle Rechtsfragen des Internets. Hrsg.: W. Lattenmayer; A. Behm. Wien: Manz, 2001. S. 79 f.

Bindungswirkung eines Anbots im allgemeinen vergleichsweise schwach und kann vor wirksamer Annahme frei widerrufen werden. Für Annahmeerklärungen gilt die „mailbox rule", d.h. eine Annahme ist im allgemeinen mit dem Absendungszeitpunkt derselben rechtsgültig.[6]

1.5 Anwendbare Rechtsordnung[7]

1.5.1 Anknüpfungspunkt

Ausschlaggebend für den Anknüpfungspunkt der anwendbaren Rechtsordnung bei internationalen Vertragsabschlüssen im Internet ist vor allem der gewöhnliche Aufenthaltsort, Wohnsitz und Sitz des Vertragspartners. In der *B2B*-Beziehung können schon konventionelle Rahmenverträge ausserhalb des Internet existieren, dann erübrigt sich diese Frage. Für den *B2C*-Bereich gilt die Verpflichtung des Anbieters, seine Anschrift vor Vertragsabschluss bekanntzugeben[8], der Konsument muss sich über die Bestellmasken hinlänglich identifizieren.

1.5.2 Rechtswahl

Bei *B2B*-Verträgen werden beide Vertragsparteien versuchen, ihr „heimisches" Recht durchzusetzen (Kollision der *AGB*). Oft wird als Kompromisslösung die Wahl des Schweizer Rechts und der Schweizer Schiedsgerichtsbarkeit vereinbart.

B2C-Rechtsgeschäfte unterliegen in Bezug auf die Rechtswahl Artikel 5 der Konvention von Rom, wonach für Konsumenten die Konsumentenschutzbestimmungen ihres Aufenthaltsstaates jedenfalls gültig bleiben, wenn der Vertragsabschluss über das Internet im Verbraucherstaat erfolgt.

Wenn keine Rechtswahl vorliegt, so gilt das UN-Kaufrecht, subsidiär das EVÜ oder weiter subsidiär das IPRG.

Das UN-Kaufrecht („Wiener Kaufrecht") gilt für Kaufverträge über Waren zwischen Vertragsparteien die in unterschiedlichen Staaten niedergelassen sind. Es gilt nicht für den Kauf von Waren für den persönlichen Gebrauch oder Gebrauch in der Familie. Die Niederlassung ist der Ort, von dem aus selbständig am Wirtschaftsleben teilgenommen wird, bei mehreren Niederlassungen gilt jene mit der stärksten Beziehung zum Vertrag.

Sachverhalte mit Auslandsberührung werden nach der Rechtsordnung beurteilt, zu der die stärkste Beziehung besteht. Das IPRG gilt nach §53 subsidiär zu zwischenstaatlichen Vereinbarungen.

---

[6] Hollmann, S.: Die elektronische Signatur. Eine rechtsvergleichende Analyse der zivilrechtlichen und zivilverfahrensrechtlichen Aspekte der elektronischen Unterschrift in den EU-Mitgliedstaaten Österreich, Deutschland, sowie den USA. – Innsbruck, Diss. 2001. S. 165ff

[7] Autengruber, S.; Lattenmayer, H.; Neuwirth, R.: Grenzüberschreitender elektronischer Handel – anwendbare Rechtsordnung. In: Aktuelle Rechtsfragen des Internets. Hrsg.: W. Lattenmayer; A. Behm. Wien: Manz, 2001. S. 112 ff.

[8] Artikel 4 Fernabsatz richtlinie 97/7/EG

Das Europäische Vertragsstatutübereinkommen ist auf *„vertragliche Schuldverhältnisse bei Sachverhalten, die eine Verbindung zum Recht verschiedener Staaten aufweisen, anzuwenden“*[9]. In Artikel 3 wird festgestellt, dass die Rechtswahl im Vertrag frei vereinbar ist. Mangels Rechtswahl gilt nach Artikel 4 das Recht des Staates, mit dem die engsten Verbindungen bestehen. Allgemeine Vermutung ist dabei, dass die engsten Verbindungen am Aufenthaltsort bzw. der Hauptverwaltung der Partei bestehen, die die charakteristische Leistung des Vertrags erbringt (Recht des Verkäufers). Artikel 5 regelt die Verbraucherverträge, d.h. Lieferungen beweglicher Sachen oder Erbringung von Dienstleistungen an Personen ohne beruflichen oder gewerblichen Zweck. Die freie Rechtswahl darf nicht zu einem Entzug des Verbraucherschutzes im Aufenthaltsstaat des Konsumenten führen wenn etwa Werbung bzw. Anbot des Unternehmens sowie die Bestellung im Aufenthaltsstaat des Konsumenten stattgefunden haben (übliche e-Commerce Rechtsgeschäfte).

2 Rechtsquellen für Sicherheitsfragen im e-Commerce

2.1 Die Richtlinie über den elektronischen Geschäftsverkehr[10]

2.1.1 Ziele der Richtlinie

Aus den Erwägungsgründen der Richtlinie lassen sich einige Zielsetzungen interpretieren. Grundsätzlich ist eine Weiterentwicklung der Dienste der Informationsgesellschaft[11] im Binnenmarkt beabsichtigt, um zu einem weiteren Abbau bestehender Schranken beizutragen. Es soll ein rechtlicher Rahmen geschaffen werden, der den freien Verkehr von Diensten der Informationsgesellschaft gewährleistet, die als *Dienstleistungen der Informationsgesellschaft* mit den Merkmalen

- in der Regel gegen Entgelt
- elektronisch im Fernabsatz
- und auf individuellen Abruf eines Empfängers erbracht

definiert sind. Verbraucher sollen Vertrauen in diese Dienste gewinnen und Rechtssicherheit genießen. Bezüglich der Vertraulichkeit ausgetauschter Daten wird auf Artikel 5 der Richtlinie

[9] Artikel 1 Abs. 1 EVÜ

[10] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“)

[11] Artikel 2 Nummer 2 der Richtlinie 98/48/EG vom 20. Juli 1998 zur Änderung der Richtlinie 98/34/EG über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften

97/66/EG hingewiesen[12], die den Mitgliedsstaaten Gesetze gegen das Abhören und Überwachen öffentlich zugänglicher Telekommunikationsnetze vorschreibt.

Nach Erwägungsgrund 61 und 62 wird auch auf die Abstimmung mit den nichteuropäischen Wirtschaftsräumen für kompatible Rechtsvorschriften und Verfahren abgezielt. Die Zusammenarbeit mit Drittländern soll im Bereich des elektronischen Geschäftsverkehrs intensiviert werden.

Laut Artikel 1 soll die Richtlinie zwecks Sicherstellung des freien Verkehrs von Diensten der Informationsgesellschaft innerstaatliche Regelungen angleichen, unter anderem kommerzielle Kommunikation und elektronische Verträge, Klagsmöglichkeiten, etc.

2.1.2 Regelungen zu Vertragsabschlüssen

Artikel 9 der Richtlinie schreibt vor, dass die Mitgliedsstaaten den Vertragsabschluss auf elektronischem Wege ermöglichen. Die entsprechenden Rechtsvorschriften dürfen keine Hindernisse für diese Verträge bilden und nicht dazu führen, dass Verträge rechtlich unwirksam oder ungültig sind, weil sie elektronisch abgeschlossen wurden. Verträge folgender Kategorien können ausgenommen werden:

- Begründung oder Übertragung von Rechten an Immobilien (ausgenommen Mietrechte)
- Die Mitwirkung von Gerichten, Behörden oder „öffentliche Befugnisse ausübende“ Berufe ist gesetzlich vorgeschrieben
- Bürgschaftsverträge und Verträge über Sicherheiten im Privatbereich
- Familienrecht und Erbrecht

Nach Artikel 10 treffen bei Bestellvorgängen den Diensteanbieter zumindest gegenüber Verbrauchern[13] Informationspflichten, wie die Bekanntgabe der technischen Schritte bis zum Vertragsabschluss, ob der Vertragstext vom Anbieter gespeichert wird oder zugänglich sein wird, die Art der Erkennung von Eingabefehlern und zur Verfügung stehende Sprachen. Der Diensteanbieter muss zumindest für Verbraucher alle ihn betreffenden Verhaltenskodizes offenlegen. Diese Informationspflichten gelten nicht bei rein individueller Kommunikation (Austausch von e-Mails). Vertragsbestimmungen und AGB müssen jedenfalls speicher- und reproduzierbar zugänglich sein. Diese Informationspflichten sind sicherlich als Beitrag zur Transparenz und zum Vertrauen in elektronische Bestellungen vor allem gegenüber Verbrauchern zu werten, da die Sicherheitsmerkmale eines Bestellvorgangs abgeschätzt werden können. Die in Artikel 11 vorgeschriebenen technischen Mittel zur Korrektur von

[12] Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation

[13] andere Parteien können abweichende Vereinbarungen treffen (z.B. Unternehmer)

Eingabefehlern vor Bestellabgabe und die Notwendigkeit einer unverzüglichen Bestellbestätigung geben zusätzliche Möglichkeiten zur Erkennung eventueller Irrtümer.

2.2 Die EU-Signaturrichtlinie[14]

2.2.1 Ziele der Richtlinie

In den Erwägungsgründen zur Richtlinie wird auf divergierende Regelungen der Mitgliedsstaaten im Bereich elektronischer Signaturen hingewiesen. Daher sollen einheitliche Rahmenbedingungen geschaffen und interoperable Produkte gefördert werden. wie in (2.1.1) wird das Vertrauen der Nutzer angesprochen sowie eine Stärkung der allgemeinen Akzeptanz der neuen Technologien. Datenschutzmaßnahmen und Schutz der Privatsphäre werden den Zertifizierungsdiensteanbietern vorgeschrieben. Der freie Verkehr im Binnenmarkt und die Freizügigkeit der Personen soll mit dieser Richtlinie unterstützt werden.

Dienste und Produkte in Verbindung mit elektronischen Signaturen sind neben der Zertifikatsverwaltung auch Registrierungs-, Zeitstempel-, Verzeichnis-, Rechner- und Beratungsdienste. Zertifizierungsdiensteanbieter sollen ungehindert grenzüberschreitend tätig sein können, um eine Steigerung der Wettbewerbsfähigkeit zu ermöglichen.

Privatrechtliche Vereinbarungen über die Verwendung elektronischer Signaturen werden nicht berührt, allerdings sollte die Zulässigkeit als Beweismittel vor Gericht nicht aberkannt werden. Auch sollen einzelstaatliche Formvorschriften für bestimmte Verträge nicht beeinflusst werden.

Zwecks Förderung der allgemeinen Akzeptanz sollen elektronische Signaturen in Gerichtsverfahren als Beweismittel verwendet werden können. Eine Anerkennung soll auf objektiven Kriterien beruhen, Vorschriften über die freie Beweiswürdigung bleiben unberührt.

Artikel 1 der Richtlinie legt den Anwendungsbereich auf die Erleichterung der Anwendung elektronischer Signaturen und einen Beitrag zur rechtlichen Anerkennung fest, wobei Abschluss und Gültigkeit von Verträgen mit bestimmten Formvorschriften und Regeln zur Verwendung von Dokumenten nicht berührt werden.

2.2.2 Elektronische Signaturen

Die Rechtswirkung elektronischer Signaturen wird in Artikel 5 behandelt, damit müssen die Mitgliedsstaaten dafür Sorge tragen, dass elektronische Unterschriften die rechtlichen Anforderungen an eine handschriftliche Unterschrift in gleicher Weise erfüllen, wenn sie

- fortgeschrittene elektronische Signaturen sind,
- auf einem qualifizierten Zertifikat beruhen,

[14] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen

- und auf einer sicheren Signaturerstellungseinheit erstellt wurden.

Die rechtliche Wirksamkeit und Zulässigkeit als Beweismittel vor Gericht darf einer elektronischen Signatur nicht allein deshalb abgesprochen werden, weil sie eine der obigen Eigenschaften nicht erfüllt oder ein nicht akkreditierter Zertifizierungsanbieter das qualifizierte Zertifikat ausgestellt hat.

Eine elektronische Signatur dient nach dieser Richtlinie der Authentifizierung, fortgeschrittene elektronische Signaturen erfüllen zusätzlich folgende Merkmale:

- ausschließlich dem Unterzeichner zugeordnet
- ermöglicht die Identifizierung des Unterzeichners
- die Erstellung erfolgt mit Mitteln, die der Unterzeichner unter seiner alleinigen Kontrolle halten kann
- eine nachträgliche Änderung der unterzeichneten Daten kann erkannt werden

Bemerkenswert ist dabei, dass an elektronische Signaturen keinerlei technische Sicherheitsanforderungen gestellt werden, sie müssen nur den elektronischen Daten beigefügt sein und der Authentifizierung dienen. Erst die fortgeschrittene elektronische Signatur erfüllt die Anforderungen an Authentizität und Integrität.

2.2.3 Qualifizierte Zertifikate

Ein Zertifikat bestätigt elektronisch die Identität einer Person, qualifizierte Zertifikate erfüllen zusätzliche Anforderungen, wie die Gültigkeitsdauer des Zertifikats, eventuelle Beschränkungen oder Begrenzungen von Transaktionswerten. Qualifizierte Zertifikate müssen durch eine fortgeschrittene elektronische Signatur des Zertifizierungsdiensteanbieters gesichert sein, der auch besondere Anforderungen erfüllen muss, wie:

- Nachweis der erforderlichen Zuverlässigkeit
- Betrieb eines schnellen und sicheren Verzeichnis- und Widerrufsdienstes
- Prüfung der Identität und spezifischer Attribute der Personen, für die qualifizierte Zertifikate ausgestellt werden
- Beschäftigung von fachlich kompetentem, qualifiziertem und erfahrenem Personal
- Einsatz vertrauenswürdiger Systeme und Produkte
- Maßnahmen gegen Fälschungen von Zertifikaten sind notwendig
- Ausreichende Finanzmittel, Haftungsrisiko muss getragen werden können
- Signaturerstellungsdaten dürfen nicht gespeichert oder kopiert werden

2.2.4 Sichere Signaturerstellungseinheit

Eine Signaturerstellungseinheit erzeugt die Signaturerstellungsdaten, d.h. private Schlüssel zur Erstellung elektronischer Signaturen. Sichere Signaturerstellungseinheiten müssen zusätzlich gewährleisten, dass:

- die Signaturerstellungsdaten praktisch einmalig sind und die Geheimhaltung hinreichend gewährleistet ist
- die Signaturerstellungsdaten nicht abgeleitet werden können und Signaturen vor Fälschungen geschützt sind
- die Signaturerstellungsdaten vor Mißbrauch durch andere geschützt sind
- die unterzeichneten Daten nicht verändert werden, eine Darstellung dem Unterzeichner gegenüber vor dem Signaturvorgang wird nicht behindert.

2.2.5 Zertifizierungsdiensteanbieter

Artikel 3 regelt den Marktzugang der Zertifizierungsdiensteanbieter. Diese brauchen keine vorherige Genehmigung, werden aber durch ein geeignetes Überwachungssystem im betreffenden Mitgliedsstaat kontrolliert. Freiwillige Akkreditierungssysteme sind erlaubt, wenn die Anforderungen an die Zertifizierungsdiensteanbieter objektiv, transparent, verhältnismäßig und nichtdiskriminierend sind. Im öffentlichen Bereich sind zusätzliche Anforderungen mit oben genannten Merkmalen definierbar.

2.2.5.1 Haftungsfragen

Artikel 6 behandelt die Haftung des Zertifizierungsdiensteanbieters, der für qualifizierte Zertifikate Geschädigten, die vernünftig auf das Zertifikat vertrauten, gegenüber haftet, dass

- zum Zeitpunkt der Ausstellung des qualifizierten Zertifikats alle enthaltenen Informationen richtig und vollständig waren und der Unterzeichner im Besitz der Signaturerstellungsdaten war, die den Signaturprüfdaten auch entsprachen.
- Die Signaturerstellungs- und Signaturprüfdaten komplementär genutzt werden können ausser der Zertifizierungsdiensteanbieter weist nach, dass er nicht fahrlässig handelte.
- Der Widerruf des Zertifikats nicht registriert wurde (Ausnahme keine Fahrlässigkeit)

Für Schäden, die über für Dritte auch erkennbare Beschränkungen des Zertifikats hinausgehen, haftet der Zertifizierungsdiensteanbieter nicht, ebenso nicht für Überschreitung eventueller Grenzen für den Wert von Transaktionen.

2.2.5.2 Datenschutzaspekte

Artikel 8 weist auf Kontrollpflichten der Mitgliedsstaaten den Zertifizierungsdiensteanbietern gegenüber hin:

- Überwachung, dass die Richtlinie 96/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr erfüllt wird.
- Überwachung, dass nur unmittelbar von betroffenen Personen oder mit ihrer ausdrücklicher Zustimmung personenbezogene Daten eingeholt werden können, die mindestens für die Ausstellung und Aufrechterhaltung des Zertifikats nötig sind.
- Eine Behinderung der Zertifizierungsdiensteanbieter an der Verwendung von Pseudonymen anstelle des Namens im Zertifikat ist untersagt.

2.2.6 Internationale Aspekte

Nach Artikel 7 müssen öffentlich ausgestellte qualifizierte Zertifikate von Zertifizierungsdiensteanbietern eines Drittstaates rechtlich denen eines Mitgliedsstaates gleichgestellt werden, wenn:

- die Anforderungen dieser Richtlinie erfüllt werden und eine Akkreditierung im Rahmen eines freiwilligen Akkreditierungssystems in einem Mitgliedsstaat erfolgte
- oder ein Zertifizierungsdiensteanbieter aus der Gemeinschaft, der selbst die Anforderungen der Richtlinie erfüllt, dafür einsteht
- oder eine Anerkennung des Zertifizierungsdiensteanbieters oder des Zertifikats im Rahmen einer bilateralen oder multilateralen Vereinbarung erfolgte

Insbesondere wird darauf hingewiesen, dass grenzüberschreitende Zertifizierungsdienste mit Drittländern und die entsprechende Anerkennung qualifizierter Zertifikate erleichtert werden soll. Die Kommission soll bei Bedarf dem Rat Vorschläge unterbreiten, die auf die Aushandlung von bilateralen und multilateralen Vereinbarungen abzielen.

2.3 Signaturgesetz und Signaturverordnung in Österreich

2.3.1 Signaturgesetz (SigG)[15]

2.3.1.1 Abweichungen von der Signaturrichtlinie

Im österreichischen SigG ist der „Signator“ auf natürliche Personen eingeschränkt, während die Signaturrichtlinie den „Unterzeichner“ als eine Person, die auch „*im Namen der von ihr vertretenen Stelle oder juristischen oder natürlichen Person handelt*[16]“, sieht. Damit findet das österreichische SigG auf juristische Personen keine Anwendung, sehr wohl aber auf deren Vertreter, die als natürliche Personen signieren. Andererseits gilt die Einschränkung auf natürliche Personen bei den Zertifizierungsdiensteanbietern nicht, mit dem Hinweis darauf, dass

[15] BG 19.8.1999 BGBl 190 über elektronische Signaturen (Signaturgesetz – SigG)
[16] Artikel 2 Nr. 3 RL 1999/93/EG

Zertifikate nicht vom Verhältnis zu handlungsbefugten natürlichen Personen abhängig sein sollen (was allerdings auch für andere juristische Personen gelten müsste). [17]

2.3.1.2 Rechtswirkungen

§3 und §4 SigG setzen die vorgaben des Artikel 5 Signaturrichtlinie vollinhaltlich um. Es werden Signaturverfahren unterschiedlicher Sicherheitsstufen zugelassen, wobei nur sichere elektronische Signaturen die rechtlichen Erfordernisse eigenhändiger Unterschriften erfüllen. Ausnahmen bestehen bei besonderen Formvorschriften, wie etwa für bestimmte Rechtsgeschäfte des Familien- und Erbrechts, bei Notwendigkeit notarieller oder gerichtlicher Beurkundung, bei Grund- oder Firmenbucheintragungen oder Bürgschaftserklärungen. Damit bedient sich der Gesetzgeber der Möglichkeit nach Artikel 1 der Signaturrichtlinie, Verträge oder rechtliche Verpflichtungen mit besonderen Formvorschriften vom Anwendungsbereich auszunehmen.

Interessanterweise erlaubt §4 Abs. 3 SigG die Anwendung der Echtheitsvermutung nach § 294 ZPO (Zurechnung der Erklärungen in einem Privatdokument zum Unterzeichner) bezüglich des Inhalts von Dokumenten, die mit einer sicheren elektronischen Signatur versehen sind. Eine elektronische Signatur dient ja nach Signaturrichtlinie und SigG lediglich der Authentifizierung des Signators obwohl aus technischer Sicht eine elektronische Signatur auch die Integrität des signierten Dokuments gewährleistet.

2.3.1.3 Anforderungen an Zertifizierungsdiensteanbieter

Aufnahme und Ausübung der Tätigkeit der Zertifizierungsdiensteanbieter bedürfen nach §6 SigG zwar keiner gesonderten Genehmigung, wie auch in Artikel 3 der Signaturrichtlinie gefordert, allerdings sind im Rahmen der Überwachung durch den Gesetzgeber einige Pflichten zu erfüllen, vor allem:

- Vorlage eines Sicherheits- und Zertifizierungskonzepts bis Aufnahme der Tätigkeit
- unverzügliche Meldung von Umständen, die Tätigkeiten zur Umsetzung dieser Konzepte verhindern

Zuwiderhandeln kann mit Geldstrafen bis zu 16.000 € geahndet werden. Die Aufsichtsstelle kann den Zertifizierungsdiensteanbietern die Verwendung ungeeigneter Technik verbieten oder gar ihre Tätigkeit ganz oder teilweise untersagen (§14 SigG). Artikel 3 der Signaturrichtlinie schreibt auch ein geeignetes Überwachungssystem für Anbieter qualifizierter Zertifikate vor, bei

[17] Stomper, B.: Das österreichische Bundesgesetz über elektronische Signaturen. In: Aktuelle Rechtsfragen des Internets. Hrsg.: W. Lattenmayer; A. Behm. Wien: Manz, 2001. S. 132 f.

anderen Zertifizierungsdiensteanbietern dürfen Mitgliedsstaaten selbst entscheiden, wie überwacht werden soll.[18]

Die Führung von Verzeichnis- und Widerrufsdiensten ist nur Anbietern qualifizierter Zertifikate vorgeschrieben (§7 SigG). Dies entspricht den Vorgaben der Signaturrichtlinie, führt aber praktisch zu großer Rechtsunsicherheit bei nicht qualifizierten Zertifikaten, da Verzeichnis- und Widerrufsdienste für die Überprüfung der Richtigkeit und Gültigkeit der Zertifikate sehr wichtig sind.[19]

2.3.1.4 Zeitstempeldienste

In §10 SigG werden Zeitstempeldienste genannt, die wie die elektronischen Signaturen in sichere und unspezifische Zeitstempeldienste eingeteilt werden, die keinen besonderen Anforderungen genügen müssen. Sichere Zeitstempeldienste müssen dasselbe Sicherheitsniveau wie sichere elektronische Signaturen aufweisen.

2.3.2 Signaturverordnung (SigV)[20]

Neben der Festlegung von Gebühren für Aufsichtstätigkeiten (§1) werden in der SigV hauptsächlich qualifizierte Zertifikate und sichere elektronische Signaturen sowie sichere Zeitstempeldienste behandelt. Es werden organisatorische und technische Standards vorgegeben, wie etwa Schlüssellängen, als sicher eingestufte Algorithmen zur Signaturerstellung, Hashverfahren (siehe 3.1) oder Formate für Signaturen und Zertifikate. Der Aufsichtsstelle wird die Installation eines Zweitsystems vorgeschrieben, das nur bei Ausfall des Hauptsystems zur Weiterführung der Signatur- und Zertifizierungsdienste verwendet werden darf.

Den Zertifizierungsdiensteanbietern werden nach §6 und §16 SigV besondere Dokumentationspflichten für ihre Systeme auferlegt.

Signatoren dürfen nach §7 nur die von den Zertifizierungsdiensteanbietern empfohlenen Datenformate, die dynamische Dokumentinhalte oder unsichtbare Daten ausschließen, zur Signierung verwenden. Die Signierfunktion darf erst nach Eingabe eines Autorisierungscodes (PIN, Fingerabdruck, ...), der nicht anderweitig auslesbar ist, ausgelöst werden.

§10 regelt Technik und Betrieb der Verzeichnis- und Widerrufsdienste für qualifizierte Zertifikate. Signatoren müssen jederzeit über einen Authentifizierungsmechanismus ihre Zertifikate widerrufen können (auch in Papierform). Widerrufe müssen jederzeit automatisiert entgegengenommen werden und dürfen nicht unbemerkt rückgängig gemacht werden können.

---

[18] ebenda, S. 141 ff.
[19] ebenda, S. 143
[20] Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung - SigV) StF: BGBl. II Nr. 30/2000

Während Verzeichnisdienste nur während der Geschäftszeiten verfügbar sein müssen, sind Widerrufsdienste durchgehend zu betreiben und ein Ersatzsystem für Ausfall bereitzustellen.

Interessant ist die Nennung einer „Sicherheitsperiode“ im Anhang bis 31.12.2005, in der die vorgeschriebenen Algorithmen und Schlüssellängen (z.B. 1023 bit bei RSA) als „sicher“ anzusehen sind.

2.4 Das UN-Modellgesetz

Das *UNCITRAL Model Law on Electronic Signatures*[21] soll zusätzliche Rechtssicherheit bei internationalen Verträgen unter Anwendung elektronischer Signaturen bringen. Im E-Sign Act (siehe 2.5) wird auf dieses Modellgesetz hingewiesen, um internationale Transaktionen zu erleichtern. Nach Artikel 3 soll ein Diskriminierungsverbot von elektronischen Signaturen gelten, wenn gewisse Mindestanforderungen erfüllt werden. Artikel 6 schreibt daher z.B. vor, dass die Signatur angemessen verlässlich sein muss. Die Signaturerstellungseinheit muss ausschließlich an den Signator „gebunden“ sein, etwaige Manipulationen müssen erkennbar sein. Signatoren und Zertifizierungsdiensteanbieter haben nach Artikel 8 und 9 bestimmte Sorgfaltspflichten zu erfüllen. Die internationale Anerkennung sicherheitstechnisch gleichwertiger elektronischer Signaturen soll nach Artikel 12 gesichert werden.

2.5 Der E-Sign Act[22] in den USA

2.5.1 Ziele und Prinzipien

Der E-Sign Act legt als allgemeines Prinzip die Äquivalenz der elektronischen mit der Papierform in Bezug auf Verträge, Unterschriften, Bekanntmachungen und anderen Aufzeichnungen fest. Grundsätzlich sind alle Transaktionen im Innen- und Außenhandel erfasst, wenn nicht explizit Ausnahmen angeführt werden. Transaktionen beziehen sich auf Unternehmen, Verbraucher und Handelsgeschäfte, ob auch E-Government erfasst ist bleibt fraglich. Die „elektronische Signatur“ ist definiert als ein elektronisches Zeichen, akustisch, symbol- oder prozesshaft, das der Unterzeichner verwendete, um einen Vertrag zu unterschreiben. Damit genügt der (bewusste) Knopfdruck auf „I accept“, ein e-Mail oder ein Telefonanruf, um ein Rechtsgeschäft abzuschließen. Fragen der Authentizität des Unterzeichners oder der Integrität des betroffenen Dokuments werden erst gar nicht berücksichtigt. Die „digitale Signatur“ wird daher zum Spezialfall der elektronischen Signatur unter Anwendung der PKI.

E-Sign knüpft prinzipiell an den Willen der Parteien an, ohne technische Standards vorzugeben. Hier ergeben sich große Unterschiede zum europäischen Modell, das die Authentifikationsfunktion der elektronischen Signatur stark betont. Lediglich auf US-

[21] URL: http://www.uncitral.org/english/texts/electcom/ml-elecsig-e.pdf am 13.5.2002
[22] “Electronic Signatures in Global and National Commerce Act“, 24.1.2000

einzelstaatlicher Ebene ergeben sich zumindest Annäherungen bei jenen Bundesstaaten, die zusätzliche konkrete technische Anforderungen stellen.[23]

2.5.2 Beweiskraft elektronischer Signaturen[24]

Elektronischen Dokumenten bzw. Signaturen darf die rechtliche Anerkennung nicht allein aufgrund der elektronischen Form abgesprochen werden. Die Echtheitsvermutung für elektronische Dokumente wird nur in einzelnen Bundesstaaten festgelegt. Das kann soweit gehen, dass die elektronische Signatur auch einer Person zugerechnet wird, wenn z.B. der Zertifikatsinhaber die „reasonable care" verletzt und ein Dritter auf die Signatur gutgläubig vertraut hat. Die Frage nach dem Umgang der Gerichte mit sicherheitstechnischen Argumenten in Streitfragen bleibt jedenfalls offen, insbesondere bei zwischenstaatlichen Fällen mit unterschiedlicher Sicherheitsinfrastruktur.

3 Technische Umsetzung und Standards

3.1 Elektronische Signatur über PKI

Im Allgemeinen basiert eine elektronische Signatur auf der Technik asymmetrischer Verschlüsselung. Diese Technik erfordert ein komplementäres elektronisches Schlüsselpaar, den privaten („private key") und den öffentlichen Schlüssel („public key"). Der private Schlüssel ist nur dem Unterzeichner bekannt und verschlüsselt den Hashwert (eindeutiger elektronischer „Fingerabdruck") des zu signierenden Dokuments.[25] Der öffentliche Schlüssel ist allgemein verfügbar, etwa durch einen Verzeichnisdienst. Durch Entschlüsselung des Hashwerts mit dem öffentlichen Schlüssel und Prüfung auf Übereinstimmung mit dem nachgerechneten Hashwert des Dokuments auf Empfängerseite weiß der Empfänger, dass

- das Dokument vom Besitzer des privaten Schlüssels unterzeichnet wurde
- und das Dokument von niemandem verändert wurde.

Der Empfänger muss allerdings noch prüfen, ob der öffentliche Schlüssel auch tatsächlich dem Signator gehört. Daher ist unbedingt eine dritte vertrauenswürdige Instanz nötig, die dafür ein Zertifikat ausstellt bzw. technisch gesehen die Übereinstimmung des öffentlichen Schlüssels mit der Identität des Signators ihrerseits elektronisch signiert. Nun weiß der Empfänger auch, dass

- der Besitzer des privaten Schlüssels dem Signator entspricht

Die Vertrauenswürdigkeit einer Zertifizierungsinstanz kann durch eine andere vertrauenswürdige Instanz mittels elektronischer Signatur bestätigt werden. Damit sind Systeme

[23] Hollmann, S.: Die elektronische Signatur. Eine rechtsvergleichende Analyse der zivilrechtlichen und zivilverfahrensrechtlichen Aspekte der elektronischen Unterschrift in den EU-Mitgliedstaaten Österreich, Deutschland, sowie den USA. – Innsbruck, Diss. 2001. S. 181

[24] ebd. S. 199ff

[25] Das Dokument selbst wird dabei gar nicht verschlüsselt und ist auch für jedermann einsehbar.

konstruierbar, in denen sich Zertifizierungsinstanzen gegenseitig authentifizieren oder aber innerhalb einer Zertifizierungshierarchie schließlich von einer zentralen Aufsichtsstelle bestätigen lassen.[26]

3.1.1.1 Sicherheitsaspekte

Der private Schlüssel darf keinesfalls nach außen gelangen, da sonst ein Missbrauch der elektronischen Signatur durch Dritte nicht auszuschließen wäre. Die Sicherheitsmaßnahmen werden sich hier vor allem auf die IT-Umgebung und Verhaltensregeln der Benutzer konzentrieren. Ein rascher Widerruf des entsprechenden Zertifikats kann hier von größter Bedeutung sein.

Der private Schlüssel ist aber auch theoretisch errechenbar, was jedoch bei Verwendung sicherer Algorithmen und geeigneter Schlüssellängen mangels Rechenleistung praktisch ausschließbar ist. Eine Schwachstelle ist jedenfalls bei der Generierung der Schlüsselpaare möglich, wenn die mathematische Nachbildung der verwendeten Reihen von Zufallszahlen gelingt. Dann können private Schlüssel leichter errechnet werden, da zumindest Wahrscheinlichkeitsverteilungen als zusätzliche Information bereitstehen.

Die gegenseitige oder hierarchische Bestätigung der Zertifizierungsinstanzen ist deshalb besonders wichtig, weil das Internet prinzipiell ein „unsicheres“ offenes Netzwerk darstellt, in dem die Authentizität von Personen oder Rechnern nicht garantiert ist. Erst das Durchlaufen einer Kette von Zertifikaten bis zu einem allgemein „vertrauten“ Zertifikat garantiert die Richtigkeit einer elektronischen Signatur. Das gilt allerdings nur dann, wenn dieses „root certificate“ nicht manipuliert wurde und eine vertrauenswürdige Zertifizierungsinstanz vorspiegelt.

3.2 Der SET-Standard

Um die Vertraulichkeit von Konto- und Kreditkarteninformationen bei Transaktionen über offene Netzwerke zu gewährleisten, wurde der SET-Standard entwickelt. Eine SET-Transaktion erlaubt die Verschlüsselung der Kommunikation Kunde-Händler-Kreditkartenunternehmen und die eindeutige Identifizierung des Karteninhabers.[27] Dabei handelt es sich allerdings um ein spezielles Verfahren zur sicheren Bezahlung über offene Netze. Technisch gesehen wird zum Signieren und Verschlüsseln ebenfalls die PKI angewendet.

[26] letztendlich muss aber zumindest einer Instanz ohne (elektronisches) Zertifikat vertraut werden, man spricht von der „root authority“, deren öffentlicher Schlüssel allgemein bekannt ist.
[27] Podovsovnik, G.; Neubauer, P.; Toch, R.: Der Vertragsabschluss im Internet. In: Aktuelle Rechtsfragen des Internets. Hrsg.: W. Lattenmayer; A. Behm. Wien: Manz, 2001. S. 98 f.

3.3 Anforderungen auf Benutzerseite[28]

In diesem Papier der TKC und TKC-GmbH vom 12.1.2000 soll der „Stand der Technik“, wie in §18 Abs. 5 SigG angesprochen, erkundet werden, um die aktuelle Erfüllung des SigG und der SigV zu prüfen. Außerdem sollen derzeit verfügbare Technologien und Fragen der Aufteilung der Verantwortung auf die Zertifizierungsdiensteanbieter einerseits und die Benutzer andererseits diskutiert werden.

3.3.1 Grundsätzliche Sicherheitsprobleme

Nach §18 Abs. 1 SigG ist die unbefugte Verwendung von Signaturerstellungsdaten verlässlich zu verhindern. Da in der Regel private Schlüssel auf den Festplatten der Benutzer abgespeichert werden kann das Kopieren und die unbefugte Verwendung nicht wirksam verhindert werden. Daher sind Hardwarelösungen für die Speicherung privater Schlüssel notwendig (Chipkarten).

Ein zentrales Problem ergibt sich aus der Forderung, dass der Signator die Kontrolle über das signierte Dokument haben muss, was hohe Anforderungen an die verwendete Software impliziert (auch wenn Chipkarten verwendet werden).

Die hohe Anzahl und Dynamik unterschiedlicher Dokumentformate, verschiedenartige Betriebssysteme und Anwendungssoftware werfen die Frage auf, ob signierte Dokumente allen Empfängern gleich dargestellt werden und ob sie verlässlich auf unbegrenzte Zeit archivierbar sind.

Die technischen Signaturverfahren lassen sich ebenso z.B. für Verschlüsselungszwecke einsetzen. Daher muss den Benutzer etwa der Unterschied zwischen der rechtsverbindlichen Signierung und der bloßen Entschlüsselung von Dokumenten klar sein.

3.3.2 Dokumentformate

Im Rahmen ständiger Erweiterungen der Funktionalität von Textverarbeitungs- und „Textanzeige“[29]-Software kam es zu einer Verschmelzung von eigentlichem Inhalt („Daten“) und dynamischen Elementen[30] („Programmen“). Selbst wenn auf reine ASCII-Texte zurückgegriffen wird, ist durch mögliche unterschiedliche Interpretation der Zeichensätze oder Steuerzeichen die bei allen Benutzern gleiche Darstellung von Dokumenten nicht garantiert.

§7 Abs. 2 SigV fordert für sichere elektronische Signaturen die Verfügbarkeit der Formatspezifikation und Nichtanwendung von dynamischen bzw. unsichtbaren Elementen, was

---

[28] Aufsichtsstelle für elektronische Signaturen (Telekom-Control-Kommission und Telekom-Control Österreichische Gesellschaft für Telekommunikationsregulierung mbH): Konsultation zu den Anforderungen des Signaturgesetzes an die Geräte der Benutzer. In: http://www.signatur.rtr.at/repository/tkc-consultation-devices-q-10-20000112-de.pdf am 14.4.2002

[29] z.B. „Acrobat Reader“ für “pdf”-Dokumente

[30] z.B. aktuelles Datum in Word-Dokumenten, diverse „plug-ins“ bei pdf-Dokumenten, eingebettete Objekte in HTML-Dokumenten, etc.

allerdings praktisch kaum vollständig realisierbar sein dürfte[31]. Die Zertifizierungsdiensteanbieter sollen bestimmte Formate festlegen, die diesen Anforderungen genügen und damit „sicher“ signierbar sind. Die Rechtsfolgen bei Unterzeichnung nicht autorisierter Dokumentformate bleiben weitgehend offen.

3.3.3 Speicherung der Signaturerstellungsdaten

Da die Speicherung privater Schlüssel auf einer Festplatte im allgemeinen nicht ausreichen wird, um Missbrauch zu verhindern, ist die Chipkarte für sichere Signaturen derzeit wohl am besten geeignet. Die sogenannten „Smart Cards“ verfügen über ein eigenes kleines Betriebssystem, das den privaten Schlüssel nach außen geheimhält. Die Sicherheitsmerkmale gehen bis in die Hardwarestrukturen, sodass eine Ableitung des Schlüssels aus dem Stromverbrauch oder einer mikroskopischen Analyse des Chiplayouts vereitelt werden kann.[32]

Nach §2 Abs. 3c SigG muss der Signator die Signaturerstellungsdaten für sichere elektronische Signaturen unter seiner alleinigen Kontrolle halten können. Dies dürfte durch eine Chipkarte mit PIN ausreichend gelöst sein, sodass der Signator nicht behaupten kann, jemand hätte unbemerkt Zugriff auf den privaten Schlüssel erlangt.

3.3.4 Vollständige Kontrolle über den Signiervorgang

Da Signiervorgänge immer teilweise über den Rechner des Signators abgewickelt werden müssen, kann auch eine verwendete Chipkarte nicht dafür garantieren, dass der Signator Kontrolle über den gesamten Prozess hat. Vor allem ist zu berücksichtigen, dass ohne Wissen des Signators etwa ein sogenannter „Trojaner“ die Kontrolle über Teile des Signiervorgangs übernommen hat, Dokumente am Weg zur Chipkarte verfälscht oder gar die Tastatureingaben des Benutzers ausspioniert und den Chipkarten-PIN verwendet oder an Dritte übermittelt. Diese Gefahrenquellen können durch einzelne Maßnahmen teilweise bekämpft werden, wie

- die Auswahl eines geeignete Betriebssystems um die versehentliche Installation von Viren oder Trojanern zu behindern.
- die Auswahl geeigneter Anwendungssoftware, die leider sehr oft grobe Sicherheitsmängel aufweist und eine „Hintertür“ für Angriffe von aussen zulassen könnte.
- spezielle Ausstattung der Chipkartenleser, sodass der PIN direkt an die Karte gesendet wird und nicht mehr über den Rechner läuft, oder direkte biometrische Erkennung.
- besondere Sicherheitsmaßnahmen der Benutzer im Umgang mit ihren Rechnern, was in der Praxis allerdings sehr beschränkt realisierbar sein wird.

[31] z.B.: das weitverbreitete Microsoft-Word Format ist dzt. nicht allgemein verfügbar.
[32] Philipp, S.: Hardwaresicherheit von Smart Card Ics,. e&i-Verbandszeitschrift des ÖVE, 2001, Heft 10, S. 477 ff.

4 Bisherige Erfahrungen

Elektronische Signaturen sind derzeit noch kaum gebräuchlich, Behörden, Banken oder Online-Shops arbeiten noch nicht mit diesen Verfahren. Beim Zertifizierungsdiensteanbieter A-Trust meint man, dass sich die elektronische Signatur „*in den nächsten zwei Jahren breit durchsetzen wird*“, Behörden, Banken und Versicherungen würden die Notwendigkeit dafür sehen. Im Herbst 2002 startet ein österreichisches Projekt für Geschäftskunden, die mittels elektronischer Signatur Überweisungen bei verschiedenen Banken online tätigen können (Ablösung des üblichen PIN-TAN-Verfahrens beim Online-Banking).[33] Bei der Aufsichtsstelle TKC sind derzeit 5 aktive Zertifizierungsdiensteanbieter registriert, die Arge Daten, A-Trust, Datakom Austria GmbH, Generali Office-Service und Consulting AG und das Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie.[34]

[33] Ruzicka, J.: Digitale Signatur soll nun forciert werden. Der Standard, 12.3.2002
[34] Liste der Zertifizierungsdiensteanbieter. In: http://www.signatur.rtr.at/de/providers/providers.html am 16.4.2002